UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,263	09/10/2003	Benedicto H. Dominguez	VISAP073	5063

22434 7590 02/10/2006

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
BAYAT, BRADLEY B	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 02/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/660,263	DOMINGUEZ ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-37,39-41 and 44-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-37,39-41 and 44-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/28/2005 has been entered.

Status of Claims

This communication is in response to remarks and amendment filed on 10/10/2005. Claims 1, 25, 37 and 52 have been currently amended. Thus claims 1-7, 9-37, 39-41 and 44-54 remain pending.

Response to Arguments

Applicant's arguments filed 10/10/2005 have been fully considered but they are not persuasive. Applicant's amendment and arguments with regards to using enrollment data as part of the authentication process to overcome the prior art is not convincing. Using enrollment, registration or subscription data as part of authentication is well known in the art. In fact, as disclosed in the background of the invention in Carrott notes, "other e-commerce payment systems require prepayments to a third-party vendor that, in turn, issues a coded credit against that deposit. Besides creating yet another layer to online transactions, these "wallet" and "Internet cash" programs also create another layer of exposure for the customer's information. Additionally, these systems require that **both the customer and merchant register to participate** in the various versions of these systems (emphasis added)." Furthermore, Tsuei

also discloses a registration process as part of its anonymous transaction system [0027, 0199-0207; fig 27 and associated text]. As taught by Tsuei, the registration/subscription data are assigned a unique identifier and coded for eventual processing and authentication. Id. Moreover, the contention forwarded by applicant that the use of registration or enrollment data to authenticate a user is novel in order to overcome the prior art is not persuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-37, 39-41 and 44-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carrott et al. (hereinafter Carrott, 6,839,692 B2), in view of Tsuei et al. (hereinafter Tsuei, US 2004/0083184 A1.)

As per Claims 1-3, 6, 7 and 41, Carrott discloses a method involving a presenter, a trusted party, and an acceptor for validating profile data of said presenter during an on-line transaction comprising:

- receiving said profile data at said trusted party (Col. 2, lines 5-10; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65);

- comparing said profile data against reference data stored by said trusted party (Col. 2, lines 5-10 and 20-33; Col. 3, lines 4-10; Col. 7, lines 4-10 and 17-25);

- notifying said acceptor by said trusted party that said profile data of said presenter is either authentic or erroneous, whereby said trusted party validates said profile data of said presenter for the benefit of said acceptor (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42).

Carrott does not explicitly disclose an enrollment process wherein authentication data is received and validated as per the customer profile.

Tsuei, however, teaches a dynamic and comprehensive system and method for processing and authentication of transactions via identified customer profiles without revealing any information the requesting party (see figure 2 and associated text, ¶12-30). According to Tsuei, once a subscriber enrolls and registers providing profile and enrollment data, a unique identifier is associated with that customer, upon matching such data and verification of the identity and credentials of the customer, notification is provided for the benefit of the requesting party over the Internet (summary of the invention, fig 2 and associated text, ¶70-74, 89-114). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Carrot's purchase transaction system to provide an anonymous transaction verification mechanism to provide security to the subscriber while at the at the same time providing further verification confirmation for the requestor.

As per claims 4 and 5, Carrott further discloses wherein the presenter and the acceptor communicate with said trusted party over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claims 9, 10, 44, 45, Carrot fails to disclose as noted above, however, Tsuei teaches a system wherein the program identity is an account number of financial account wherein the trusted third party maintains said account (fig 12-17, 20 and associated text). It would have

been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include a program identity number such as an account number, unique identifier or other code of some sort issued and stored by the trusted party so that the trusted party has a unique number or code associated with the presenter as taught by Tsuei et al and which may be used later to identify the presenter or an account maintained by the trusted party.

As per claims 11-12 and 14-17, Carrott et al further disclose initiating communications between the presenter and acceptor and receiving profile data and a program identity number at the acceptor for the presenter (Col. 4, lines 5-18; Col. 5, lines 25-38). Carrott et al, however, fail to explicitly disclose receiving identity data at the acceptor. Tsuei et al disclose a method for verifying the identity of on-line credit card purchasers and further teach receiving, at a trusted party, authenticating data from the presenter; comparing, by the trusted party, the authenticating data against pre-designated authenticating data previously designated for the presenter and notifying the acceptor by the trusted party that the identity of the presenter is either authentic or erroneous, whereby the trusted party authenticates the identity of the presenter for the benefit of the acceptor (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claim 13, Carrott et al further disclose querying the trusted party by the acceptor whether account data updating can be provided (Col. 2, lines 25-33).

As per claims 18 and 20-21, Carrott et al further disclose transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party validate said profile data of said presenter as discussed above. Carrott et al, however, fail to disclose requesting that the third party authenticate the identity of the presenter. Tsuei et al disclose a method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 23-24, Carrott et al further disclose providing, by the trusted party, of updated profile data when the profile data is determined to be out of date (Col. 2, lines 25-33, see also updating disclosed in Tsuei).

As per claims 19, 22, 48 and 51, Carrott et al and Tsuei et al disclose transmitting a data authentication response message from the trusted party to the acceptor, however, fail to transmit this message via the presenter. Examiner takes Official Notice, however, that routing authentication response messages to an acceptor such as a merchant via a presenter such as a purchaser is well known in the art and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to route the message in this fashion depending upon the configuration and desired message routing.

As per claims 25, 27, 52 and 54, Carrott et al disclose an on-line data authentication system comprising:

- a trusted party who receives, validates and provides profile data of a presenter (Figure 1; Col. 2, lines 5-10 and 20-33; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65; Col. 7, lines 4-10 and 17-25); ;

- an acceptor who conducts a transaction with said presenter and who requests said trusted party to validate said profile data of said presenter (Figure 1; Col. 6, lines 60-67; Col. 7, lines 1-10); and

a directory server configured to determine the existence of said trusted party who will be able to validate said profile data of said presenter (Col. 6, lines 60-67; Col. 7, lines 1-10).

Carrott et al further disclose local user authentication wherein the user inputs a user ID and password which is then verified by the users computer prior to proceeding (Col. 5, lines 57-63; Col. 6, lines 20-25). Carrott et al, however, fail to explicitly disclose receiving authentication data at a trusted party during an enrollment process in which enrollment data is used to verify the

authenticity of said presenter, and an acceptor requesting the trusted party to authenticate the identity of the presenter. Tsuei et al disclose a method for verifying the identity of on-line credit card purchasers and further teach receiving during an enrollment process, at a trusted party, authenticating data from the presenter; comparing, by the trusted party, the authenticating data against pre-designated authenticating data previously designated for the presenter; and notifying the acceptor by the trusted party that the identity of the presenter is either authentic or erroneous, whereby the trusted party authenticates the identity of the presenter for the benefit of the acceptor (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 26 and 53, Carrott et al further disclose wherein the presenter and the acceptor communicate with said trusted party over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claim 28, Carrott et al fail to disclose as above, however, Tsuei et al disclose receiving and storing authenticating data from the presenter at the trusted party wherein the authenticating data becomes the pre-designated authenticating data (fig 2, 12-20 and associated

text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include receiving and storing, at the trusted party, authenticating data of the purchaser as pre-designated authenticating data for purposes of authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 29-30, Carrott et al fail to disclose, however, Tsuei et al disclose providing, by the trusted party, to the presenter a program identity number which is correlated with the identity, profile data and authenticating data and storing the program identity number by the trusted party (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include a program identity number such as an account number, unique identifier or other code of some sort issued and stored by the trusted party so that the trusted party has a unique number or code associated with the presenter as taught by Tsuei et al and which may be used later to identify the presenter or an account maintained by the trusted party.

As per claims 31-32, Carrott et al disclose a request message transmitted from the acceptor to the trusted party via a directory server, the message containing a query as to whether the trusted party will be able to validate the profile data of the presenter (Col. 6, lines 45-67) and

a response message for validating the profile data of the presenter (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42). Carrott et al, however, fail to disclose transmitting a message to the third party querying the third party as to whether the third party will be able to authenticate the identity of the presenter. Tsuei et al disclose a method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claims 33-36, Carrott et al disclose a request message transmitted from the acceptor to the trusted party via a directory server, the message requesting that the trusted party validate the profile data of the presenter, the request message including profile data of the presenter (Col. 2, lines 5-10; Col. 3, lines 4-10; Col. 4, lines 8-18; Col. 5, lines 25-38 and 55-67; Col. 6, lines 60-65) and a response message for validating the profile data of the presenter and whether or not the profile data is accurate or contains errors (Col. 2, lines 5-10 and 20-33; Col. 7, lines 24-42). Carrott et al, however, fail to disclose transmitting a message to the third party requesting that the third party authenticate the identity of the presenter. Tsuei et al disclose a

method for requesting that the trusted party verifying the identity of on-line credit card purchasers and further teach notifying the acceptor that the identity is authentic when the data matches (fig 2, 12-20 and associated text, ¶12-30, 70-158). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Carrott et al and include authenticating the identity of the purchaser as taught by Tsuei et al so that the merchant is ensured that the purchaser is the authorized user for the credit card. Tsuei et al provides motivation by indicating that there is a need for a method or system for verifying the identity of an on-line purchaser, and ensuring to a reasonable extent that the purchaser is in fact the party authorized to use the credit card presented for payment.

As per claim 37, Carrott et al disclose a method involving a presenter, a trusted party, and an acceptor for providing at least some profile data of said presenter during an on-line transaction to said acceptor comprising:

- querying said trusted party by said acceptor for said trusted party to provide said profile data to said acceptor (Figure 2; Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34); and

- providing profile data of said presenter, by said trusted party, to said acceptor (Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34).

As per claims 39-40, Carrott et al further disclose wherein the presenter, acceptor and trusted party communicate over the Internet (Abstract; Figure 1; Col. 3, lines 45-55; Col. 8, lines 10-15).

As per claim 46, Carrott et al further disclose wherein the identity and profile data include at least the name and address of the presenter (Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34).

As per claims 47 and 50, Carrott et al further disclose transmitting a data authentication request message from said acceptor to said trusted party in order to request that said trusted party provide said profile data of said presenter (Figure 2; Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34); and transmitting a data authentication response message from said trusted party to said acceptor, said data authentication response message containing said profile data of said presenter (Col. 2, lines 20-33; Col. 5 line 60-Col. 6 line 3; Col. 7, lines 24-34).

As per claim 49, Carrott et al fail to disclose, however, Tsuei et al disclose requesting the presenter, by the trusted party, for the authenticating data (fig 2, 12-20 and associated text, ¶12-30, 70-158). Carrott et al, however, fail to disclose asking the presenter, by the trusted party, for permission to provide the profile data of the presenter to the acceptor. Examiner takes Official Notice, however, that utilizing a third party entity to essentially filter customer personal or profile data provided to merchants based on permissions controlled by the customer is well known in the art and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the reference to Carrott et al and include the ability to filter the information provided to the merchant. One would have been motivated to filter this type of

customer personal or profile data since it was well known at the time of applicant's invention that consumers were generally concerned about divulging personal or private information.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US PAP 2002/0023059 A1 to Bari et al.
- "Novell Debuts New DIGITALME 'In the Net' Service, dated October 5, 1999.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

Bradley B. Bayat, Esq.
Art Unit 3621
February 6, 2006